# 1.0 PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to provide the steps to be followed to create the centralized AWS native backup plan and to add new OU/functional account or the instances of Linux and Windows operating systems in appropriate backup plan and to restore the backup in AWS landscape.

# 2.0 SCOPE

|  |  |
| --- | --- |
| **Regions,**  **Functional Areas,**  **Job Functions** | This SOP applies to,   * Regions: Global * Functional Area: IT Technology * Job Functions: Personnel supporting the backup and restore activities in the scope of this document |
| **Applications** | This SOP applies to,   * Amazon Elastic Compute Cloud (EC2) Linux instances * Amazon Elastic Compute Cloud (EC2) Windows instances |
| **Limitations** | This SOP does not apply to,   * Any other AWS services * On-Prem services |

# 3.0 DELEGATION OF ACTIVITIES

Activities required to execute this SOP may be delegated to an individual with the proper education, experience, and training to successfully execute the activity. The party responsible retains full responsibility for the outcome of any delegated activity.

# 4.0 RESPONSIBILITIES AND PROCEDURE

<Client Name> will use AWS Backup as the tool for managing backup and restore for EC2 Windows and EC2 Linux instances. During build phase, EC2 instances are added to the backup policy.

Periodic verification of the backup and restore, including bi-annual restore testing, will be part of the overall Landing Zone periodic review process.

**4.1. CREATING A BACKUP PLAN / NAMING CONVENTION**

|  |  |  |
| --- | --- | --- |
| Responsible Role |  | Activity |
| Cloud Operations Engineer |  | Create an IAM role to AWS Backup to assume and perform backup and restore operations using the Cloud formation template as per Appendix 4. |
|  |  | Create a backup policy, backup plan and backup rules as per Appendices 1 and 2. |
|  |  | Add Targets to the backup policy as per Appendix 3. |

**4.2. ON-DEMAND BACKUP**

|  |  |
| --- | --- |
| Responsible Role | Activity |
| Application Owner | Create a ticket using <Ticketing tool name and URL for the service catalog to open backup request> |
| Cloud Operations Engineer | * Review and verify the request. * Create the on-demand backup with requested retention as per Appendix 5 |

**4.3. RESTORE PROCESS**

|  |  |
| --- | --- |
| Responsible Role | Activity |
| Application Owner | Create <ticketing tool name> ticket for restore |
| Cloud Operations Engineer | * Review and verify the request. * Create the on demand restore with requested instance ID as per Appendix 6. * Verify that the restored instance is accessible via AWS Console/ SSM and Okta ASA * Inform the application owner to check and confirm. |
| Application Owner | * Check the connectivity to the restored resource * Verify that the application is functioning as expected * Confirm the status to CloudOps Engineer |
| Cloud Operations Engineer | Report <ticketing tool name> the status and close the ticket |

**4.4. DELETE BACKUP PLAN**

|  |  |
| --- | --- |
| Responsible Role | Activity |
| Cloud Operations Engineer | Create <ticketing tool name> Change Request for Deletion of the backup plan. |
| Change Approver | Review and approve the change request |
| Cloud Operations Engineer | * Delete backup plan as per Appendix 7 once the change request is approved. * Report the status and close the ticket. |

**4.5. BACKUP MONITORING AND REPORTING**

|  |  |
| --- | --- |
| Responsible Role | Activity |
| Cloud Operations Engineer | Monitor failed backup jobs with Cloud Watch metrics/SNS topic as per Appendix 8. |
| Cloud Operations Engineer | Review backup reports stored on AWS Console on daily basis and perform appropriate action such as re-submitting backups. |
| Cloud Operations Engineer | * Verify backup status on AWS backup service dashboard. * Create a <ticketing tool name> Incident ticket for backup failure in IT Service Management (ITSM) - Incident Management. |
| Cloud Operations Engineer | Share a weekly backup report to ECS Operations Lead. |

**4.6. PERIODIC VERIFICATION FOR RESTORE**

|  |  |  |
| --- | --- | --- |
| Responsible Role | Activity | |
| Cloud Operations Engineer | Perform bi-annual backup and restore verification in <Client name> environment, as part of periodic verification.   * Create ticket for restore testing * Applications are chosen from each AWS region. Only Non-PROD environments will be used to conduct testing. | |
| Responsible Role |  | Activity |
|  |  | In case of any failures, the test run will be failed, and defect will be logged in  <ticketing tool>. |
|  |  | Troubleshooting will be performed to identify the reason for failure. |
|  |  | For any issues in AWS Backup process/ tool or at the application level, incident will be logged. AWS will be engaged for the issues in the tool, if required. |

**4.7. BACKUP MEDIA**

Backup of media used to store backups is managed by AWS and was reviewed as part of the AWS Supplier

# 5.0 REVISION HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Effective Date | Description of Changes |
| 1.0 | Current | Initial version |
| 2.0 |  |  |
| 3.0 |  |  |

# 6.0APPENDICES

|  |  |
| --- | --- |
| 1. | Appendix 1: Backup Schedule |
| 2. | Appendix 2: Creation of Backup Policy |
| 3. | Appendix 3: Attaching Targets to The Backup Policy |
| 4. | Appendix 4: IAM Role for Aws Backup |
| 5. | Appendix 5: Steps to Create On-Demand Backup |
| 6. | Appendix 6: Steps to Restore A Backup |
| 7. | Appendix 7: Steps to Delete Backup Plan |
| 8. | Appendix 8: Steps to Monitor Backup |

**APPENDIX 1: BACKUP SCHEDULE**

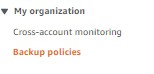
Following is the backup schedule and retention policy that will be applied in <client name> landscape, unless there is an application specific need that arises, and such requirement is approved by application team.

|  |  |  |
| --- | --- | --- |
| **Backup Type** | **Schedule** | **Retention** |
| Daily (Production Tier 3 and 4) | 11:00 PM Regional time | 45 days |
| Every 4 Hrs (Production Tier 1 and 2) | 00:00, 04:00, 08:00, 12:00, 16:00 and 20:00 hrs  (Regional time) | 45 days |
| Weekly (Non-production) | Friday 11:00 PM Regional time | 45 days |

**APPENDIX 2: CREATION OF BACKUP POLICY**

**A: Backup policy - Prod (Backup policies are created in Organization master account)**

1. Create the required IAM role to AWS Backup to assume and perform back-up and restore operations using the Cloud formation template (refer Appendix 4 for steps).
2. Navigate to AWS backup service using the following link [https://console.aws.amazon.com/backup.](https://console.aws.amazon.com/backup)
3. In the left navigation pane, choose Settings to open the Backup policy page.



1. Enter the Policy name in accordance to <CLIENT NAME> naming convention <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_POLICY
2. Enter the policy description with Backup plan details
3. Select the Visual editor in the configure backup plan section
4. Enter the Backup plan name

<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_PLAN

1. Select the Backup plan region as required (Example: us-east-1)
2. Navigate to Backup rules section in Visual editor
3. Click add backup rule
   * Enter the rule name [<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_RULE]
   * Specify the region specific backup vault (example: PROD-NAM-BACKUP\_VAULT)
4. Select the schedule frequency = “DAILY“
5. Specify the Backup window with following parameters
   * Backup window start time: 11.00 PM Local time
   * Start within: 1 hour
   * Completes within : 8 hour
6. Select the Life cycle policy of the backup with following parameters
   * Transition to cold storage: Never
   * Expires after: 45 days
   * Select copy to destination region option (example: US West(Oregon)) and select destination Backup vault (example: <CLIENT NAME>-PRD-USWest-BACKUP\_VAULT ).
7. In Advanced settings,
   * Select transition to cold storage: Never

Retention period: 45 days

1. Select the Assign Resources section and enter the Resource assignment group name

[<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_ASSIGNMENT\_GROUP]

1. Specify the IAM role created with backup full access policy
2. Assign the Tag with target KEY and VALUES

KEY: environment-id

Value: prod

Or

KEY: RecoveryTier

Value: Tier3 or Tier4

1. Click Add assignment
2. Click create policy
3. Verify the JSON parameters for the configuration compliance.

**B: Backup policy with remote region replication-Prod (Backup policies are created in Organization master account)**

1. Create the required IAM role to AWS Backup to assume and perform back-up and restore operations using the Cloud formation template (refer Appendix 4 for steps)
2. Login to the member account and select the secondary region (example: ‘us-west-2’)
3. Access ‘AWS Backup’ service and select Backup Vault
4. Create Backup vault Example:

Name: <CLIENT NAME>-PRD-USWest-BACKUP\_VAULT

Encryption key: AWS/Backup

1. Login to AWS master account, select region (For Example: US-East-1) and access backup service
2. Access backup policies and click on create backup policy

*Name: <CLIENT NAME>-PRD-NAM-Tier1-BACKUP\_POLICY*

*Policy description: Backup policy for Tier1 Application with remote region replication*

1. In configure backup plan session, update below details,

Backup Plan Name: <CLIENT NAME>-PRD-NAM-Tier1-BACKUP\_PLAN

Backup Plan region: US-EAST-1

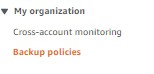
1. In Add backup rule session, update below details,
   * Backup rule Name: <CLIENT NAME>-PRD-NAM-Tier1-BACKUP\_RULE
   * Specify the region specific backup vault (example: NONPROD-NAM-BACKUP\_VAULT).
   * Backup frequency: Custom cron expression: cron (0 0,4,8,12,16,20 ? \* \* \*)
   * Start within: 1 Hour
   * Complete within: 4 Hour
   * Transition to cold storage: never
   * Retention period: 45 days
   * Select copy to destination region option (example: US West(Oregon)) and select Destination Backup vault (example: <CLIENT NAME>-PRD-USWest-BACKUP\_VAULT)
2. In Advanced settings,
   * Select transition to cold storage: Never
   * Retention period: 45 days
3. In resource assignment session update below parameters,
   * Resource assignment name: <CLIENT NAME>-PRD-NAM-Tier1-BACKUP\_RESOURCE\_ASSIGNMENT1
   * IAM Role: BackUpCrossAccountRole For Example:

Resource tag key: APP\_ID Tag values: APP-43125 or

1. Save the policy
2. Open policy again and select target and click on attach
3. Navigate to applicable member account and attach to policy.

**C: Backup policy for Non-Prod environment (Backup policies are created in Organization master account)**

1. Create an IAM role to AWS Backup to assume and perform back-up and restore operations using the Cloud formation template
2. Navigate to AWS backup service using the following link [https://console.aws.amazon.com/backup.](https://console.aws.amazon.com/backup)
3. In the left navigation pane, choose Settings to open the Backup policy page.



1. Enter the Policy name in accordance to <CLIENT NAME> naming convention <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_POLICY
2. Enter the policy description with Backup plan details
3. Select the Visual editor in the configure backup plan section
4. Enter the Backup plan name <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_PLAN
5. Select the Backup plan region as required (example: us-east-1)
6. Navigate to Backup rules section in Visual editor
7. Click add backup rule, enter the rule name [<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_RULE] 11. Specify the region specific backup vault (example: NONPROD-NAM-BACKUP\_VAULT).
8. Select the schedule frequency = “Weekly“
9. Specify the Backup window with following parameters
   * + Backup window start time: 11.00 PM Local time (Friday)
     + Start within: 2 hours
     + Completes within : 1 day
10. Select the Life cycle policy of the backup with following parameters
    * + Transition to cold storage: Never
      + Expires after: 45 days
11. Select the Assign Resources section, enter the Resource assignment group name .

[<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_ASSIGNMENT\_GROUP]

1. Specify the IAM role created with backup full access policy
2. Assign the Tag with target KEY and VALUES

KEY: environment-id

Value: dev or test

1. Click Add assignment
2. Click create policy
3. Verify the JSON parameters for the configuration compliance

**APPENDIX 3: ATTACHING TARGETS TO THE BACKUP POLICY**

* 1. Navigate to AWS backup service using the link <https://console.aws.amazon.com/backup>
  2. In the left navigation pane, choose Settings to open the Backup policy page
  3. Select the Backup Policy created in APPENDIX 2
  4. Navigate the Targets section in Backup policy
  5. Click attach to attach the targets (OU’s) / accounts
  6. Select the list of OU’s / accounts to be added as a target for the Backup policy created in Appendix 2.

Additional Notes:

* 1. As mentioned in section Appendix 2 - step 17, a tag must be attached to the server in order to for it to be enrolled in the backup schedule.
  2. Verify the new resource id in AWS backup to confirm that new instance is added to backup. Every server will be onboarded to AWS backup during build phase

**APPENDIX 4: IAM ROLE FOR AWS BACKUP**

AWS backup service needs an exclusive IAM policy as a prerequisite that allows it to connect with other services in AWS such as EC2 and EBS. This IAM role needs to be created as a onetime requirement in AWS master account and will grant permission to AWS Backup service to access EC2 in the backend across AWS organization unit.

* 1. Launch an AWS CloudFormation StackSet in the master account.
  2. Provide a **StackSet name** as **AWS Backup configuration US EAST**.
  3. Enter **BackUpCrossAccountRole** in **IAM Configuration**. Choose **Next**.
  4. Choose **Service managed permissions** to allow automatic deployment of this IAM role to any new accounts that are added to the target OUs in future. Choose **Next**.
  5. Choose **Deploy to organization**. Choose **US East, Frankfurt and Tokyo** in **Specify regions**. Keep other default settings. Choose **Next**.
  6. Select the check box for **I acknowledge that AWS CloudFormation might create IAM resources with custom names.** Choose **Submit** and verify the stack sets deployment completion under the **Stack Instances** tab.

## APPENDIX 5: STEPS TO CREATE ON-DEMAND BACKUP

In the event an On-Demand backup is needed or requested, AWS backup console allows for that. The request must include the instance ID and retention period required.

The Cloud Operations will perform the following steps.

1. From AWS backup select create on-demand backup option.
2. Select the resource type and search with resource id to select the resource to backup
3. Select ‘Create backup now’ option
4. Select expiry as requested in the ticket request
5. Choose default vault and backup IAM role
6. Click on create on-demand backup and verify the job for completion.

## APPENDIX 6: STEPS TO RESTORE A BACKUP

For a backup restore, an Application owner will raise a restore request in <ticketing tool>. The request must include the instance ID and the date from which the restore to be done.

To restore a specific image, Cloud operations team will:

1. Select the backup vault and search with instance ID (resource ID) which will list available AWS recovery point that can be restored.
2. Select the specific required date image and click on restore (*This action will restore the data to original location and hence it is important user or application owner approval is mandatory before a restore action is executed*)
3. Verify the restore job status form Job’s session and ensure completion

## APPENDIX 7: STEPS TO DELETE BACKUP PLAN

To delete a backup plan, an appropriate risk review and change approval must be performed before any action is taken. Implementation of the backup plan deletions includes:

1. Click on AWS backup/ Backup plan
2. Select the backup plan to delete
3. Type the backup plan to confirm and delete the plan.

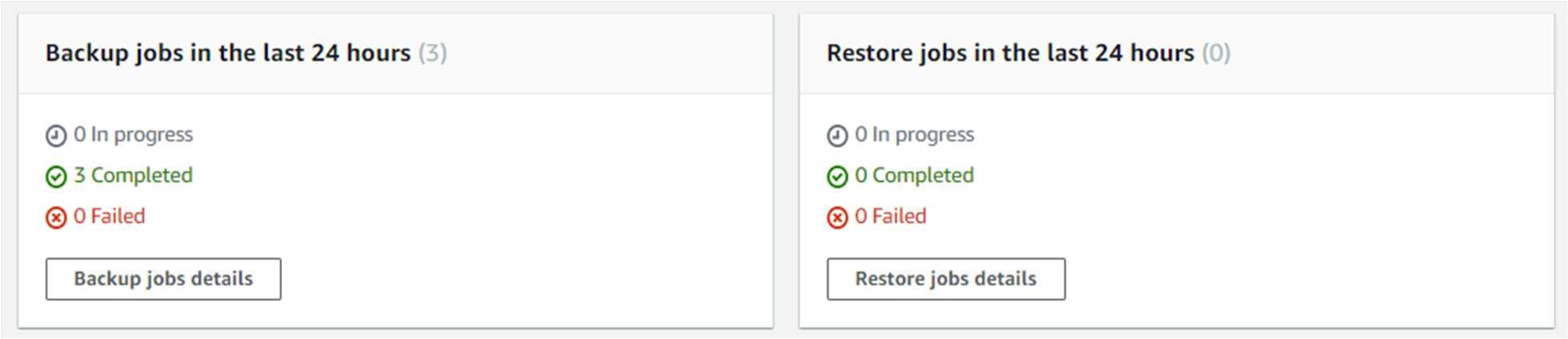
## APPENDIX 8: STEPS TO MONITOR BACKUP

AWS Backup provides a dashboard that makes it simple to audit backup and restore activity across AWS services. Cloud Ops will view the status of recent backup jobs and restore jobs across AWS services. AWS Backup integrates with AWS CloudTrail, which provides a consolidated view of backup activity logs that make it quick and easy to audit what and how resources are backed up. AWS Backup will be integrated with Amazon Simple Notification Service (SNS), which automatically alert the Cloud Ops team on backup activity, such as when a backup fails or a restore is initiated.

Backup reports will be reviewed on daily basis and an appropriate action such as re-submitting backups or trouble shooting issues in environment will be performed.

For Backup reports:

* Login to AWS console for each account and region, select AWS backup service Dashboard
* Review the backup status in last 24 hours
* If there are failed jobs, create a <ticketing tool name> Incident ticket for backup failure
* Cloud Operations team to share a weekly backup report



For failed jobs alert, Create the CloudWatch alarm with below metrics:

|  |  |
| --- | --- |
| Metric Name | : Backup => NumberOfBackupJobsFailed |
| Threshold | : > 1 |
| Period (Mins) | : 5 |
| Datapoint | : 1 out of 1 |